**HW 2 CMSC 456. Morally DUE Sep 28**
**SOLUTIONS**
**NOTE- THE HW IS FIVE PAGES LONG**

1. (0 points)

   (a) What is the day and time of the midterm?

   (b) What is the day and time of the final?

   (c) What is the *dead-cat policy*?

   (d) What is the *mask policy*?

**GOTO NEXT PAGE**

2. (20 points) Alice and Bob are going to use the Vig cipher. The keyword is *Kunal.* Alice wants to send

   *Bill's Ramsey Theory course is Awesome!*

   What does Alice send?

   Make it in blocks-of-five capital letters, though since its 32 letters it will be 6 blocks of 5 and then 2 letters.

   You can either

   - do this by hand,
   - write a program to do it for you, or
   - find software on the web to do it for you. If you do this then on the HW include the website of the software you used. ALSO say if the software you used leaked any information.

   **SOLUTION**

   I used

   `https://cryptii.com/pipes/vigenere-cipher`

   to initially get

   *Lcyl'd Buzspi Nuezbs pofbmr id Kqrszwy*

   I then removed the punctuation and made all of the letters capital and put it into blocks of 5.

   *LCYLD BUZSP INUEZ BSPOF BMRID KQRSZ WY*

   The software I used was terrible- it left in caps vs small letters, and spacing, which leaks a lot of information.

   **END OF SOLUTION**

**GOTO NEXT PAGE**

3. (20 points) Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are relatively prime to $n$. EXAMPLES

   $\phi(5) = 4$ since all the four elements $\{1, 2, 3, 4\}$ are rel prime to 5.

   $\phi(p) = p - 1$ for any prime $p$.

   $\phi(15) = 8$ since $\{1, 2, 4, 7, 8, 11, 13, 14\}$ are the elements in $\{1, \ldots, 15\}$ that are rel prime to 15.

   NOTE: If $p$ is s prime then $p$ is rel prime to all $p - 1$ elements of $\{1, \ldots, p - 1\}$ and hence $\phi(p) = p - 1$.

   And now finally the problem

   We will determine $\phi(143)$ without having to look at all of the numbers. We will need to factor $143 = 11 \times 13$. Note that a number is rel prime to 143 if it has *neither* 11 *nor* 13 as a factor.

   (a) (5 points) How many numbers in $\{1, \ldots, 143\}$ have 11 as a factor. DO NOT do this by listing them all out. Show your work.

   **SOLUTION**

   Note that $\frac{143}{11} = 13$.

   $1 \times 11$, $2 \times 11$, ..., $13 \times 11$

   all have 11 as a factor. So the answer is 13.

   **END OF SOLUTION**

   (b) (5 points) How many numbers in $\{1, \ldots, 143\}$ have 13 as a factor. DO NOT do this by listing them all out. Show your work.

   **SOLUTION**

   Note that $\frac{143}{13} = 11$.

   $1 \times 13$, $2 \times 13$, ..., $11 \times 13$

   all have 13 as a factor. So the answer is 11.

   **END OF SOLUTION**

   (c) (5 points) How many numbers in $\{1, \ldots, 143\}$ have 11 AND 13 as a factor. DO NOT do this by listing them all out. Show your work.

   **SOLUTION**

   $11 \times 13 = 143$. This is the only number that has 11 AND 13 as a factor.

   **END OF SOLUTION**

(d) (5 points) Using the information from the last three parts, and the law of inclusion-exclusion, find $\phi(143)$.

**SOLUTION**

Let $A$ be the elements of $\{1, \ldots, 143\}$ that have 11 as a factor. From the above $|A| = 13$.

Let $B$ be the elements of $\{1, \ldots, 143\}$ that have 13 as a factor. From the above $|B| = 11$.

From the above $|A \cup B| = 1$.

The numbers that DO have a factor in common with 143 either have 11 or 13 as a factor. By the law of inclusion and exclusion there are

$$|A| + |B| - |A \cup B| = 13 + 11 - 1 = 23$$

numbers that DO share a factor with 143.

Hence there are $143 = 23 = 120$ that DO NOT.

So $\phi(143) = 120$.

NOTE also that $\phi(143) = \phi(11 \times 13)$, but also note that $\phi(11) = 10$ and $\phi(13) = 12$. So $\phi(11 \times 13) = \phi(11) \times \phi(13)$.

**END OF SOLUTION**

(e) (0 points) Let $p, q$ be two primes. Give a formula for $\phi(pq)$ in terms of $p$ and $q$. Show your work.

**SOLUTION**

We count the number of elements in $\{1, \ldots, pq\}$ that DO share a factor with $pq$.

The number of elements of $\{1, \ldots, pq\}$ that have $p$ as a factor is $q$.

The number of elements of $\{1, \ldots, pq\}$ that have $p$ as a factor is $p$.

The number of elements of $\{1, \ldots, pq\}$ that have $p$ and $q$ as a factor is 1.

Hence the number of elements of $\{1, \ldots, pq\}$ that share a factor with $pq$ is

$$p + q - 1.$$

Hence the number of elements of $\{1, \ldots, pq\}$ that DO NOT share a factor with $pq$ is

$$pq - (p + q - 1) = (p - 1)(q - 1) = \phi(p)\phi(q).$$

**END OF SOLUTION**

**GOTO NEXT PAGE**

4. (20 points) Alice and Bob are using the Keyword-Shift Cipher with key the phrase

*Mayim Bialik should host Jeopardy*

and shift 1.

(a) (7 points) Give the table that Alice uses to ENCODE messages.

**SOLUTION**

We write the phrase but remove repeated letters and make all letters small.

*mayiblkshoudtjepr*

We first write the table without the shift.

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| m | a | y | i | b | l | k | s | h | o | u | d | t |

| n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| j | e | p | r | c | f | g | n | q | v | w | x | z |

We would then shift by 1, which we OMIT.

**END OF SOLUTION**

(b) (7 points) Give the table that Bob uses to DECODE messages.

**SOLUTION**

OMITTED

**END OF SOLUTION**

(c) (6 points) If Alice wants to send the message below, what does she send? (The answer should be in blocks of 5 all capitals.)

*Almost all students have been vaccinated*

**SOLUTION**

OMITTED

**END OF SOLUTION**

(d) (0 points- do not hand in) Does the ENCODE and DECODE tables look like this is a randomly generated permutation of $\{A, \ldots, Z\}$ OR are there signs that it came from the keyword-Shift Cipher?

**SOLUTION**

OMITTED.

**END OF SOLUTION**

**NOTE ON GRADING** All three parts will be graded either 0 or full credit. If you get part 1 wrong and this leads to part 3 being wrong, we will get 0 on both parts. We will not check if YOUR part 3 is consistent with YOUR part 1. Hence **be careful and double check**.

**GOTO NEXT PAGE**

5. (40 points) Do the programming assignment that is just below this hw on the website and is labeled *Programming Assignment for HW 2*.